The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/10/2010

SUBJECT:
Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (MS10-088)

OVERVIEW:
Two new vulnerabilities have been discovered in Microsoft PowerPoint, a program used for creating presentations. These vulnerabilities can be exploited by opening a specially crafted PowerPoint file received as an email attachment, or by visiting a web site that is hosting a specially crafted PowerPoint file. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Microsoft Office XP
- Microsoft Office 2003
- Microsoft Office 2004 for Mac
- Microsoft PowerPoint Viewer Service

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Two new vulnerabilities have been identified in Microsoft PowerPoint that could allow remote code execution.

PowerPoint Parsing Buffer Overflow Vulnerability
A vulnerability exists in the way that Microsoft PowerPoint parses a specially crafted PowerPoint 95 file. Please note that this vulnerability is rated moderate by Microsoft because Office 2003 SP3 will not open PowerPoint 95 files by default and newer versions of Microsoft Office are not affected by this vulnerability.

PowerPoint Integer Underflow Causes Heap Corruption Vulnerability
This vulnerability is caused by the way Microsoft PowerPoint parses a specially crafted PowerPoint File.

These vulnerabilities can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted PowerPoint presentation as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted PowerPoint presentation that is hosted on the page.
Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is currently no patch available for this vulnerability for Microsoft Office 2004 for Mac.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-088.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2572
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2573

Security Focus:
http://www.securityfocus.com/bid/44628
http://www.securityfocus.com/bid/44626